Organizational Information	Response
Organization Name	Mikrodots, Inc.
Organization Sector	Legal Technology
Organization Size	10
Organization Website	http://www.mikrodots.com
Organization Background	Mikrodots, Inc. is a legal tech firm in Boston, Massachusetts providing outsourced technology support for New England law firms.
Point of Contact Information	**Response**
POC Name	Michael Doherty
POC E-mail	mdoherty@mikrodots.com
POC Phone	781-932-6655

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Mikrodots, Inc.: As a Legal Tech firm providing outsourced IT support to law firms, we realize cybersecurity education and an iterative cybersecitiy process is needed for the New England law firms we support. The midsize law firms do not generally have cybersecurity staff and rely on outsourced technology providers like Mikrodots to lead their cybersecurity initiatives.	http://www.mikrodots.com
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	Mikrodots is a framework user who supports multiple organizations who are not using the Framework directly. The framework supports our iterative cybersecurity process, which we delliver to our clients.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Mikrodots uses the framework as the foundation for our iterative cybersecurity program and evaluation tools that can be consumed by our managed services clients.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The Core is very useful in developing our cybersecurity self evaluation tool, and the profile helps our clients determine their risks and priorities.	
5	What portions of the Framework are most useful?	The Profile is the starting point for our clients. It is most useful to develop awareness and establish risk tolerance and directed actions. The core is most useful to our organization to educate internal employees and to develop a cybersecurity strategy with our clients.	
6	What portions of the Framework are least useful?	Implementation Tiers	
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	Lack of awareness. Targeted towards federal and utilities, not general businesses.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	Undefined as of this date.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	Better definitions and cross references of applicable requirements, standards and processes. Continued cooperation with ISO, BSI, COBIT and the like.	
10	Should the Framework be updated? Why or why not?	Yes, it should be a living document that keeps pace with the evolving cybersecurity environment and new technology uses such as Internet of Things and the proliferation of Bring Your Own Device.	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.		
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?		
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	Legal sector and financial sectors SEC: https://www.sec.gov/investment/im-guidance-2015-02.pdf	

#	Question Text	Response Text	References
14	Should developments made in the nine areas identified by NIST in its Framework-related Roadmap be used to inform any updates to the Framework? If so, how?	Yes, through review and RFI, following change management best practices.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Maintain the core principles and definitions while making changes. Follow change management process, RFI and make changes over a reasonable time frame.	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	Yes, the web resources, CFS Core spreadsheet and linked resources form the base of our client questionnaire and helped in the development of the our profile tool.	
17	What, if anything, is inhibiting the sharing of best practices?	Need and easy way and common location to share.	
18	What steps could the U.S. government take to increase sharing of best practices?	Review, define and publish best practices. Best practices are referred to several times ("and additional best practices", "industry best practices", "best practices of risk management") but are not defined with regards to cybersecurity.	
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	peer-recognition and trade associations, possibly certifications	
20	What should be the private sector's involvement in the future governance of the Framework?	Continued private sector involvement and cooperation with the NIST is imperative to the adoption of the framework.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Should be either all or none.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	See 21	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?		
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?		
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?		